CERTIFIED PUBLIC MANAGER PROJECT

Enterprise Risk Management (ERM): "A Journey, Not a Destination"

Submitted by Frankie B. Ramsey
Manager Internal Audit
South Carolina State Housing Finance and
Development Authority
300-C Outlet Pointe Blvd.
Columbia, SC 29210
www.schousing.com

Frankie.Ramsey@SChousing.com (803) 896-9279 Fax-(803) 551-4977

February 3, 2014

CONTENTS

Enterprise Risk Management (ERM):
"A Journey, Not a Destination"

Introduction

South Carolina State Housing Finance and Development Authority (herein referred to as "SC Housing") is moving to adopt consistent and holistic approaches to risk management. SC Housing management recognizes that risk management is a management process that should be fully integrated with the management of the organization. Enterprise risk management (ERM) – or more properly enterprise-wide risk management is one such approach to managing risk. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [1] defines it as "*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*" A comprehensive risk management framework provides an end-to-end link between objectives, strategy, execution of strategy, risks, controls, and assurance across all levels in the organization.

In the fall of 2011 Internal Audit (IA), an independent, objective assurance and consulting function within the SC Housing, piloted an enterprise-wide risk management (ERM) program that includes using control self-assessment (CSA) to accomplish the agency's overall ERM objectives. "CSA is a formal documented process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met. The responsibility for the process is shared among all employees

[1]The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization, established in the US, dedicated to providing thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, ERM, fraud, and financial reporting.

within an organization. CSA is conducted within a structured environment in which the process is thoroughly documented and the process is repetitive as an incentive for continuous improvement. (Underline added for emphasis) The CSA process allows management and/or work teams directly responsible for a business function to:

* Evaluate risk
* Participate in the assessment of internal control
* Develop action plans to address excessive risk, and
* Assess the likelihood of achieving business objectives

In addition, CSA is a process that generates information on internal control that is useful to management and internal auditors in judging the quality of control."[2]

Pursuant to the CSA Sentinel article titled "Reflections on the First 20 Years of CSA" published by the Institute of Internal Auditors (IIA)[3] in 2007, "Today, traditional CSA workshops are being conducted in more the 50 countries across the world. Practitioners are experimenting with the process tool to inquire into traditionally difficult soft areas. Ethics, governance, health and safety, enterprise risk management, and teamwork have all become accessible using this flexible and people-oriented approach." CSA often paves the road for an organization to explore and embed enterprise wide risk management where the risk control framework of the organization is continuously monitored and optimized.

Within the SC Housing CSA is primarily conducted through Internal Audit facilitated workshops and participant surveys. This approach is designed to improve the SC Housing's control environment by:

---

[2] Professional Practices Pamphlet 98-2 "A Perspective on Control Self-Assessment" The Institute of Internal Auditors, pg. 4

[3] Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs Fla.; USA. The IIA is the internal audit acknowledged leader, chief advocate and principal educator.

- Increasing employee awareness of organizational objectives and the role of internal control in achieving goals and objectives, and
- Encouraging personnel to carefully design and implement control processes and continually improve operating control processes.

Our first workshop explains how to self-assess internal control over a department's significant activities and processes that impact strategic, operations, financial reporting, and compliance objectives. The second workshop helps participants assess the control environment, the flow of information and communication. The third workshop is designed to aid the department's employees in identifying and scoring significant risks and determining the appropriate controls to mitigate those risks. The fourth workshop provides a format for group discussion of the significant risks; identifying control deficiencies; and reporting results to executive management.

Since beginning our ERM journey in the fall of 2011, Internal Audit has facilitated control self-assessments in four of SC Housing's business units: SC HELP Program, Finance and Procurement Division, the Development Division and the Investor Services Division. The control self-assessment process has three phases: (1) the review phase, (2) testing phase, and (3) reporting phase. To date, SC Housing control self-assessments have only addressed the review and reporting phases. The review phase is primarily aimed at ensuring that internal control is properly designed to manage risks which threaten business objectives to within a prudently acceptable level, or risk appetite. During this phase division staff, assisted by IA, documented divisions' mission, objectives, assessed the control environment, risk assessment, control activities, information and communication, ongoing monitoring activities, identified control deficiencies, and proposed corrective action(s) to remedy the deficiencies for each significant activity (or process) in the division. After documenting the review phase, division management reports the results to Executive Management (reporting phase). The control self-assessment

report has four elements: (1) Memorandum to Executive Management, (2) Control Self-Assessment Action Plan (3) Control Environment & Information and Communication Survey Results, and (4) Internal Auditors' Report.

Problem Statement

While conducting risk assessment is typically considered a "one time activity," in the context of ERM it is continuous and on-going part of the daily responsibility of managers and employees throughout the organization. Presently, the SC Housing does not have a defined process framework (infrastructure) to facilitate the advancement of risk management capabilities on an on-going basis. Without having such a defined process framework (infrastructure) to facilitate the advancement of risk management capabilities over time, (2nd year and beyond) and to assist management stay on course with the mission and objectives it has charted, the SC Housing's ERM journey will risk being short lived… one and out after completion of the 1st year's initial four CSA workshops facilitated by IA.

The goal of this project is to research and identify techniques, methods, frameworks, and/or tools that can help advance the SC Housing's ERM/CSA objectives by enabling CSA *to be a consistently applied management driven self-assessment process applied across the entire SC Housing to include testing of internal controls, (CSA phase three) performing annual control self-assessments, and assurance reporting on the design adequacy and effectiveness of controls.*

As I begin this CPM project I am reminded of the advice offered by two leading professionals with broad backgrounds in leading control self-assessments and frequent authors, course leaders, and speakers for the IIA and other professionals. In his book Control Self-Assessment: A Practical Guide, Larry Hubbard, CIA, CPA, CCSA cautions "…*In practice, very few audit departments have fully transferred CSA ownership to Work teams*." Dave Harmon, in the CSA Sentinel article titled "The End of an Era": Q&A with Dave Harmon, he exclaims: "*For*

CSA to truly live up to its potential, the methodology needs to become management's tool. Management must embrace CSA as a management practice, taught by management, with support from audit departments. As long as CSA is considered to be part of auditing, I think it will have limits placed upon it. So, my advice to CSA proponents is to light many fires, but understand that many will burn out. And stay optimistic. To borrow a line from the Rolling Stones, you can't always get what you want, but if you try sometimes, you just might find ... you get what you need from CSA. CSA will continue on in an altered role and like everything else, will change and evolve over time."

Data Collection & Analysis

Data collection and analysis for this project consist primarily of two components: First, researching ERM/CSA primarily through review and analysis of literature aimed at helping organizations move up the maturity curve in their ongoing development of robust ERM and CSA processes. Literature reviewed includes: COSO's Enterprise Risk management - Integrated Framework Executive Summary 2004, IIA publications and position papers including but not limited to: CSA Sentinel "The End of an Era, "Embracing Enterprise Risk Management"-- Practical Approaches for Getting Started, Professional Practices Pamphlet 98-2: A perspective on Control Self-Assessment, Risk Management-Frequently Asked Questions, Protiviti Inc., Guide to Enterprise Control Self-assessment: A Practical Guide, etc. Refer to Appendix I for a complete list of all the sources used in researching this project. The other component of data collection and analysis consists of brainstorming sessions with SC Housing's Internal Audit Director and Development Division Quality Control Manager to determine what the SC Housing's future ERM/CSA process should resemble including, but not limited to: roles and responsibilities for management and staff , self-assessment frequency and documentation requirements, and tools for use in conducting self-assessments.

Data Collection

-Enterprise Risk Management (ERM) -

"Few companies have implemented ERM, as defined by COSO…While some companies have begun their journey to implement ERM; few of them have completed it."[4] "COSO states that ERM is 'a means to an end, not an end in itself.' The trend towards ERM recognizes that risks are complex and interrelated, and the business environment isn't getting any simpler. Therefore, there are significant benefits that can be achieved from evaluating and managing risk on a comprehensive enterprise-wide basis. The process of implementing ERM is fundamentally a process of education, building awareness, developing buy-in and ultimately assigning accountability and accepting ownership. (Underline added for emphasis) Because risks will continue to change and evolve as the global marketplace changes and evolves, implementing ERM should be viewed as a commitment to continuous improvement as opposed to an event."[5] (Underline added for emphasis) "The COSO framework states that the CEO 'is ultimately responsible and should assume ownership' over the implementation of ERM… Support from the top is vital to an effective functioning ERM infrastructure. To create and sustain momentum, senior management must demonstrate a strong commitment to ERM through consistent communications and actions. Whether through the executive committee, or other, resolution of the process ownership questions for critical risks is one of the most important tasks in implementing ERM."[6] "The ERM journey is a growth process, which leads the firm to improve its risk management capabilities. As it navigates its ERM journey, the organization becomes

---

[4]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Questions 10 "Why have companies that have tried to implement ERM failed?

[5]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Questions 13, "What Does it mean to "implement ERM"

[6]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Questions 40, "Must the CEO be fully engaged in the ERM Process or system for it to be successful, or can he or she delegate it to someone else?

more sensitive to changes in the environment and within its business processes. This sensitivity in the culture is important because opportunities and risk will continue to surface and change rapidly in the global economy. Thus developing an effective, enterprise-wide view of business risk management will always be a journey of continuous learning and improvement."[7] "A comprehensive, enterprise-wide focus on managing risk is a high implementation standard for most companies because of the behavioral changes required to overcome the conventional management of risk in silos, which companies have had in place for a long time. For that reason, in recent years ERM has been pursued more by visionary organizations than by the mainstream of companies. ERM is a 'best-of-breed' approach consisting of different techniques that different companies have implemented in different ways"[8] Dave Harmon said in a September 2008 CSA Sentinel article "Q&A with Dave Harmon: "*...the issue with enterprise risk management (ERM) is not so much how to do it. Generally, the ERM implementation process is pretty well understood. It's determining how to adapt ERM to the existing organizational culture that poses the biggest problem.*" ERM is not a "one-size-fits-all" solution on a shelf. According to COSO, "*management must decide the nature of the ERM solution based on the organization's size, objectives, strategy, structure, culture, management style, risk profile, industry, competitive environment and financial wherewithal.*"

-Objectives, Risks, and Controls -

A comprehensive risk management framework provides an end-to-end link between objectives, strategy, execution of strategy, risks, controls, and assurance across all levels in the

---

[7]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Questions 138 "What is program management and why is it relevant to ERM implementation?

[8]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Question 5 "Which companies are implementing ERM"?

[9] Control Self-Assessment (CSA) Workshop Participant's Guide, SC Housing, page 6 revised 2/7/12

[10]Enterprise Risk management—Integrated Framework—Executive summary September 2004, pg. 6

organization. "...Setting objectives is a precondition to internal control. If an organization does not have objectives, there is no need for internal control... A clear set of objectives is fundamental to the success of a department. Specifically, a department should have (1) a mission statement, (2) written objectives for the department as a whole, and (3) written objectives for each significant process in the department."[9] Internal control is an integral part of enterprise risk management[10] and who hasn't heard by now that management, not the internal audit department, is responsible for the internal controls in their organizations? The SC Housing's Executive Director has echoed this message to CSA workshop participants when she states *"...An important message to be communicated is that internal control is, to some degree, everyone's responsibility. Therefore, I encourage you to participate actively in the workshops, to perform a thorough control self-assessment, and to take steps to ensure that internal control within SC State Housing is adequately designed, properly executed, and effective."* In other words, within SC Housing, management at the department level is primarily responsible for, and is accountable for internal control in their department. "The central theme of internal control is (1) to identify risks to the achievement of an organization's objectives and (2) to do what is necessary to manage those risks."[11] Once an organization has determined the desired capabilities for managing a given risk and has successfully implemented those capabilities, it must be ever vigilant about improving them continuously as facts and circumstances change and the risk of significant external and internal events occurring in the future evolves.

To this point in the SC Housing's ERM/CSA journey we have done the things which are necessary to complete the review phase of the self-assessment process – we have reviewed the control environment, risk assessment, control activities, information and communication, and

[9] Control Self-Assessment (CSA) Workshop Participant's Guide, SC Housing, page 6 revised 2/7/12

[10] Enterprise Risk management—Integrated Framework—Executive summary September 2004, pg. 6

[11] SC Housing Control Self-Assessment (CSA) Workshop Participant Guide, pg. 6 revised 2/7/12

ongoing monitoring activities for each significant activity (or process) in the divisions for which IA has facilitated a CSA workshop. We have identified control deficiencies and proposed corrective action to remedy the deficiencies—we have answered the question "Is internal control adequately designed?

-Testing Internal Control-

An entity's enterprise risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, new technology, changes in entity structure or direction, or the introduction of new processes or steps within a process. In the face of such changes management needs to determine whether the functioning of enterprise risk management continues to be effective. To answer the following question "Is internal control properly executed?" controls must be tested. Once a decision is made to test internal controls, when practical, testing should be performed by employees who are independent of the activity being tested. Employees, like auditors, don't have to look at every single piece of information to determine that the controls are functioning and should focus their monitoring activities in medium to high-risk areas. (Risks or survey results with inherent risk scores between 9 & 25) **Note: (**Risk significance is rated on a scale of 1(low) to high (25) and is the product of the risk consequence score (1-5) multiplied by the risk likelihood score (1-5)**)** The use of spot checks of transactions, basic sampling techniques, inquiry, observation, re-performance of control activities and examining evidence to support legal compliance can provide a reasonable level of confidence that the controls are functioning as intended.

During the "Review Phase" of our control self-assessment division staff identified "key controls" for each risk associated with a process or activity in our Risk Control Worksheet

(RCW)[12] The intent of the RCW is to document responses to the inherent risks identified in achieving the Authority's objectives and to document our consideration of residual risks and the effectiveness of control activities. The decision to test controls rests with senior management and is based on factors such as: 1) Significance of the risk score and the strength of the control necessary to reduce the risk within management's risk appetite; 2) How long the control has been in operations; 3) The use of monitoring controls, and 4) Frequency of internal or other audits of the control. In most cases, it will not be prudent or practical to attempt to test every control identified as a "key control". Instead, management should identify and focus their testing on the "Primary" key control(s). The primary control(s) is the predominate control activity in reducing the risk score relative to all control activities that reduce the risk score to within our appetite. In some cases there will be more than one primary key control. Primary controls selected for testing should be identified and marked ☑ on the RCW. In addition to using the RCW to document our testing of control activities, the RCW should also be used to document testing in the control environment and information and communications component of the authority's internal control system where survey results gave rise to proposed actions to mitigate negative survey responses.

-Roles and Responsibilities-

"While ultimate responsibility for ERM starts at the top, everyone who matters within an organization should participate to some extent in the ERM process. While several executives have significant responsibilities for ERM, including the chief risk officer, chief financial officer, chief legal officer, and chief audit executive, the ERM process works best when all key managers of the organization contribute. The COSO framework states that managers of the

[12]Control Model Implementation: Best Practices by James Roth PHD; CIA pg. 31 defines the risk/control matrix as an analytical tool in matrix format with one column for risk and one or more columns for controls. The risk control matrix (referred to as RCW at the SC Housing) drives the risk assessment thought process. It is a disciplined tool that can encompass "soft" as well as hard controls. Appendix VIII

organization 'support the entity's risk management philosophy promote compliance with its risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances.' Therefore, identifying leaders throughout the organization and gaining their support is critical to successful implementation. A goal of ERM is to incorporate risk management into the organization's agenda and decision-making processes. This means that ultimately, every manager is responsible, which can only happen when performance goals are clearly articulated, and the appropriate individuals are held accountable for results."[13] A common leading practice involves assigning risk ownership and accountability to specific senior managers. Clear roles and responsibilities, along with common definitions for risk language enable a consistent and comprehensive approach to addressing organizational risk.

Data Analysis

ERM is not a "one-size-fits-all'' solution on a shelf. According to COSO, management must decide the nature of the ERM solution based on the organization's size, objectives, strategy, structure, culture, management style, risk profile, industry, competitive environment and financial wherewithal. There is overwhelming unanimity among ERM practitioners and proponents that the process of implementing ERM is fundamentally a process of education, building awareness, developing buy-in, and ultimately assigning accountability and accepting ownership. Two of the most critical success factors noted were leadership support – having a key sponsor and management and board buy-in to the self-assessment program. Third ranked success factor - adequate training to help lead the way to implementation and maturity. SC Housing has a key sponsor, Director of Internal Audit (Chief Audit Executive) along with management and board buy-in. SC Housing has developed adequate training for implementing

[13]Guide to Enterprise Risk Management: Frequently Asked Questions, Protiviti Inc. January 2006: Questions 13, "Who should participate in the ERM process and how?

ERM; however, much work still remains with regards to the training that will be required in order to move us along the ERM maturity continuum. Because risks will continue to change and evolve, implementing ERM should be viewed as a commitment to continuous improvement as opposed to an event. Consequently, developing an effective enterprise-wide view of business risk management will always be a journey of continuous learning and improvement. A review of the literature revealed only one off-the-shelf type tool that was considered to be useful in advancing our ERM/CSA objectives -- a matrix tool "Assessing an organization's risk maturity" (Refer to Appendix IX). Additionally, for this CPM project I developed a "Control Self-assessment Checklist" for use by management in conducting and documenting annual control self-assessments. (Refer to Appendix III) This tool was developed primarily in consultation with the Director of Internal Audit and Development Division's Divisional Risk Officer. Along with the Control Self-Assessment Checklist, I also developed three (3) examples of memorandums for use by the Division Director and Divisional Risk Officer for communicating to staff the parameters for conducting an annual control self-assessment. Refer to Appendices IV, V, and VI.

Implementation Plan

Internal Audit is aware the implementation of ERM may take many years to achieve the highest maturity level of "Risk enabled" – that is, risk management and internal controls are fully embedded into the operations. (Refer to Appendix IX –Risk Maturity Assessment Tool) Further, Internal Audit recognizes that each SC Housing division's culture is unique and that division resources are varied, as well as limited. As such, a tailored approach will be required for facilitating the advancement of risk management capabilities over time for each division and to assist management stay on course with the mission and objectives it has charter. This tailored approach necessitates IA meeting with divisions' management in order to identify gaps to the division's ERM maturity utilizing the Risk Maturity Assessment Tool – Appendix IX. Once

gaps are identified division management will prepare a documented plan for updating their risk assessment. This plan is to describe at minimum, the division's approach for assessing whether or not changes in processes, personnel, technology, laws and regulations, or others have occurred since the initial IA facilitated CSA, whether or not new risks have emerged or been identified, whether or not controls are in place to manage those risks or additional controls are required to be implemented in order to manage risks within our risk appetite, internal control testing scope, e.g., which internal controls are to be tested, by whom, over what timeframe, and identification of staff participating in the assessment.

Evaluation Method

The IIA's International Standards for the Professional Practice of Internal Auditing (Standards) is essential in meeting the responsibilities of internal auditors and the internal audit activity. Standard 2120 –Risk Management requires that "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." The Standard goes on to state "Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management and the board to carry out their responsibilities.

Additionally, Standard 2130-Control require that "The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. The internal audit activity must evaluate the

adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems.

Summary

Given the evolutionary nature of ERM and the dynamic nature of risk, the ERM process must be ongoing and not viewed as a one-time event. The initial risk assessment process will need periodic updating and SC Housing will need to be attuned to the need in identifying new and emerging risks. Now that ERM is off the ground, the Authority can look for additional ways to expand the implementation of ERM across the enterprise. We are aware that, while tangible risk processes may have been implemented during this initial phase of ERM deployment, the processes may likely fall short of a complete ERM process and need to be enhanced. Accordingly, the Authority's risk management leader (Director of Internal Audit, Chief Audit Executive) need to continue to drive further development and maturity of the risk management processes.

Above all, let us keep in mind the benefits of taking small, incremental steps on the path toward full ERM rather than attempting to implement the complete ERM framework all at once. The goal is to keep the momentum for ERM that will continue to expand and deepen the Authority's ERM capabilities on a continual basis.

APPENDICES
INDEX

Appendix I

BIBLIOGRAPHY

- Professional Practices Pamphlet 98-2, *A perspective on Control Self-Assessment*, (The Institute of Internal Auditors), 1998

- Control Self-Assessment: A Practical Guide By Larry Hubbard, CIA, CPA, CCSA, (The Institute of Internal Auditors), 2005

- Control Model Implementation: Best Practices By James Roth, PHD, CIA, (The Institute of Internal Auditors), 1997

- Special Report "Contemporary Practices in Risk Management" -- Implementation ideas from leading companies , (The Institute of Internal Auditors), January 2012

- Committee of Sponsoring Organizations of the Treadway Commission "Thought Leadership in ERM"-- Risk Assessment in Practice by Deloitte & Touche LLP, Dr. Patchin Curtis and Mark Carey, October 2012

- Committee of Sponsoring Organizations of the Treadway Commission "Thought Leadership in ERM"—COSO's 2010 Report on ERM—Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework By Mark S. Beasley, Bruce C. Branson and Bonnie V. Hancock, December 2010

- Committee of Sponsoring Organizations of the Treadway Commission "Thought Leadership in ERM"—Embracing Enterprise Risk Management—Practical Approaches for Getting Started By Mark L. Frigo and Richard J. Anderson, January 2011

- Committee of Sponsoring Organizations of the Treadway Commission-- Internal Control—Integrated Framework—Guidance on Monitoring Internal Controls, Introduction, January 2009

- Committee of Sponsoring Organizations of the Treadway Commission—Enterprise Risk Management—Integrated Framework—Executive Summary, September 2004

- Committee of Sponsoring Organizations of the Treadway Commission "Thought Leadership in ERM"—Risk Assessment in Practice, October 2012

- Committee of Sponsoring Organizations of the Treadway Commission –The 2013 COSO Framework & SOX Compliance—One Approach To An Effective Transition By J. Stephen McNally, CPA 2013

- Risk Based Internal Auditing – Three views on implementation, by David Griffiths PHD, march 15, 2006, page 48-51 (Refer to Appendix IX)

Appendix I

BIBLIOGRAPHY

- ERM Initiative at NC State University "Report on the Current State of Enterprise risk Oversight" Management accounting Research conducted on Behalf of the American Institute of CPAs By Mark Beasley, Bruce Branson, Bonnie Hancock 2009

- Guide to Enterprise Risk Management—Frequently Asked Questions, Protiviti Inc. Independent Risk Consulting, January 2006

- International Standards for the Professional Practice of Internal Auditing (Standards), Issued October 2008 Revised: October 2012, The Institute of Internal Auditors –Standard 2120-Risk Management and 2130-Control

- Statements on Management Accounting, Enterprise Risk and Control "Enterprise Risk Management: Tools and Techniques for Effective Implementation, Institute of Management Accountants, 2007

- State of Tennessee—Management's Guide To Risk Management and Internal Control, August 2007

- The "CSA Sentinel" is a retired electronic newsletter published by the Institute of internal Auditors originally created to support the development of knowledge surrounding the implementation of control self-assessment workshops and techniques and enterprise risk management (ERM) methodologies.

    - Third Quarter 2007 * Vol. 11* No. 3 – Feature article: Reflections on the First 20 Years of CSA

    - First Quarter 2007 * Vol. 11* No. 1 – Feature article: Moving Toward a Global CSA Standard

    - Third Quarter 2006 * Vol. 10* No. 3 – CSA at BellSouth: The Afterlife

    - Second Quarter 2006 * Vol. 10* No. 2 – Feature article: Control Self-assessment: Defeating the "Killer Bees to Group Dynamics"

    - Vol. 10* No. 1* February 2006 – The CSA Practitioner: Teacher, Student, Partner Wrapped into one

    - Vol. 6* No. 3* October 2002 – The Road to ERM

    - Vol. 5* No. 2* June 2001 – A Journey Beyond Internal Control

COMMON ERM/CSA LANGUAGE AND GLOSSARY OF TERMS

- **Control Activities**...The policies and procedures that help to ensure that actions identified as necessary to manage risks are carried out properly and in a timely manner.

- **Control Self-Assessment (CSA)**.... A technique developed in 1987 at Gulf Canada that is used by a wide range of organizations including corporations, charities and government departments, to assess the effectiveness of their risk management and control processes. Since its introduction the technique has been widely adopted in the United States, European Union and other countries. There are a number of ways a control self-assessment can be implemented but its key feature is that, in contrast to a traditional audit, the tests and checks are made by staff whose normal day-to-day responsibilities are within the business unit being assessed. The CSA process allows management and/or work teams directly responsible for a business function to:

  - Evaluate risk
  - Participate in the assessment of internal control
  - Develop action plans to address excessive risk, and
  - Assess the likelihood of achieving business objectives

- **CSA Action Plan**...One of four elements of the Control Self-Assessment Report. It summarizes action plans to address excessive risks, including internal control proposed and actual implementation dates, risk scores, name of implementer, Internal audit verification of implementation, etc.

- **CSA Report**.... After the review and/or testing phase has been documented, department management reports the results to Executive management (has four elements: (1) Memorandum to Executive Management, (2) Control Self-Assessment Action Plan (3) Control Environment & Information and Communication Survey Results, and (4) Internal Auditors' Report.

- **Consequence (Impact)**.... The effect that the risk would have on the organization's ability to successfully achieve its objectives if the risk occurs.

COMMON ERM/CSA LANGUAGE AND GLOSSARY OF TERMS

- **Divisional Risk Officer (DRO)**...Division staff member responsible for coordinating Division's annual CSA and the on-going monitoring activities which: (1) track implementation of proposed actions/key controls, (2) either validate or invalidate the design, execution and effectiveness of internal control.

- **Enterprise-wide Risk Management**.... A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." *As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)*

- **Inherent Risks**.... The risk in a business or process before the effect of any risk mitigation, control or transfer activities.

- **Internal Control**...A process effected by board and management of an organization designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (1) Effectiveness and efficiency of operations, (2) Reliability of financial reporting, and (3) Compliance with applicable laws and regulations. Generally speaking there are two types: preventive and detective controls. Both types of controls are essential to an effective internal control system.

    - Preventive Controls are designed to discourage errors or irregularities from occurring. They are proactive controls that help to ensure departmental objectives are being met.
    - Detective Controls are designed to find errors or irregularities after they have occurred.

- **Internal Control Process**...Internal control consists of five interrelated components as follow:

    - **Control Environment**.
    - **Risk Assessment**.
    - **Control Activities**
    - **Monitoring**
    - **Information & Communication**

- **Objectives**: What an entity desires to achieve in alignment with the entity's mission and overall strategy.

COMMON ERM/CSA LANGUAGE AND GLOSSARY OF TERMS

- **Process...** It involves steps and decisions in the way work is accomplished, and may involve a sequence of events.

- **Process Outline**... A control and risk assessment tool used to document key process steps, including who performs each step, where, when, and how performed, applications used, process inputs and outputs, process name, owner, date prepared and/or updated etc. **(Refer to Appendix VII)**

- **Process Owner**...Person who has ultimate responsibility for the performance of a process in realizing its objectives and has the authority and ability to make necessary changes.

- **Likelihood**.... The probability that exposure to a risk will occur.

- **Mitigation**... To moderate or decrease the likelihood or potential impact of exposure to a risk.

- **Residual Risks**.... The risks remaining after the application of controls.

- **Risk**.... The potential for loss or failure to meet business objectives as a consequence of internal or external events.

- **Risk Assessment**...The identification and analysis of risks to the achievement of operations, financial reporting, compliance and strategic objectives forming a basis for determining how those risks should be managed.

- **Risk Appetite**.... The expression of the level of acceptable and/or unacceptable risk as defined by the Commission and senior management.

- **Risk/Control Worksheet**...A control and risk assessment tool for: identification and analysis of risks to the achievement of objectives, identification of objectives, identification of existing and proposed controls for mitigation of risks, documentation of risk significance (score) before and after application of controls, (inherent and residual risks), and test of controls documentation. **(Refer to Appendix VIII)**

- **Risk Management...** A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

COMMON ERM/CSA LANGUAGE AND GLOSSARY OF TERMS

- **Risk Owner**...The person who has the highest interest in the risk being correctly treated – and who has the right level of authority to treat the risk accordingly.

- **Risk Register –** A schedule or table capturing the list of significant risks facing the organization.

- **Risk Significance (Score)**... Risk significance is rated on a scale of 1 (low) to high (25) and is the product of the risk consequences score (1-5) multiplied by the risk likelihood score (1-5). Risk scores (inherent or residual) of 4 or less are within the risk appetite and require no further management or mitigation.

SC HOUSING
CONTROL SELF-ASSESSMENT CHECKLIST

Appendix III

DIVISION NAME: _____
PROGRAM NAME: _____
SIGNIFICANT PROCESS: Refer to Division-wide Process Register
ASSESSMENT COMPLETION DATE: _____

INTRODUCTION:

While conducting risk assessment is typically considered a "one time activity," in the context of enterprise risk management (ERM) it is continuous and on-going, part of the daily responsibility of managers and employees throughout the organization.

An Organization's ERM changes over time. Risk responses that were once effective may become irrelevant; risks previously unidentified have surfaced; control activities may become less effective, or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, changes in entity structure or direction, or the introduction of new processes and/or technology. In the face of such changes management needs to determine whether the functioning of enterprise risk management continues to be effective.

INSTRUCTIONS:

This checklist has been designed as a tool to assist SC Housing management and staff in conducting and documenting effective and efficient annual control self-assessment of division risks and controls. The checklist is aligned with criteria established in "Enterprise Risk Management-Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission.

Each question should be answered by a check mark in the appropriate column (Yes, No, or N/A). The questions have been prepared so that a positive answer will indicate an effective self-assessment. A negative (No) answer will indicate a deficiency in the self-assessment and require respondent to include notation regarding what action, if any, is being or will be taken to address the issue.

This control self-assessment checklist has been prepared and reviewed as follows.

Prepared by: _____ Date: _____

Approved by: _____ Date: _____

The checklist is divided into six major sections:

Section	Title
I	Mission/Objectives
II	Process Outlines
III	Risk Control Worksheets (RCW)
IV	Control Self-Assessment Action Plan
V	Staff Training
VI	Report to Executive Management

SC HOUSING
CONTROL SELF-ASSESSMENT CHECKLIST

Appendix III

DIVISION NAME: _____

PROGRAM NAME: _____

SIGNIFICANT PROCESS — Refer to Division-wide Process Register

ASSESSMENT COMPLETION DATE: _____

Section I - Division Mission/Objectives

Section I is designed to document management's review of the division's mission, and objectives for accuracy, currency, and completeness.

		Yes	No	N/A	Comments
1.0	The division's mission, and objectives havebeen established, reviewed for currency, accuracy, & completeness, and have been effectively communicated to all program staff.				
2.0	Division level objectives are supportive of the agency-wide level objectives presented in the strategic plan.				
3.0	Written procedures designed to support the achievement of the program objectives have been established and/or updated, communicated, and practiced so that people understand what is expected of them and the scope of their freedom to act.				
4.0	Measurable performance targets and/or indicators have been developed and are being tracked for program objectives.				

Section II - *Significant* Processes/Process Outlines/Division-Wide Process Register

Section II is designed to document review of significant processes by managers or process owners to ensure: All significant processes and process outline steps have been identified, and the process outline remains current, accurate, and complete

		Yes	No	N/A	Comments
1.0	Have all significant division level processes been identified and reviewed for currency, accuracy, & completeness, and been effectively communicated to all program staff.				
2.0	Has each step of the "Process Outline" been reviewed/updated/clarified as appropriate by owner and appropriate program staff using "Track Changes"? Date: January 14, 20xx				
3.0	Has each column of the Process Outline been annotated for each step?				
4.0	Division-wide Process Register has been reveiwed to ensure: 1) all activities listed agree with process outlines; 2) all process tab # have been hyperlinked to the respective Process Outline; 3) all RCW Tab #s have been Hyperlinked to the respective RCW; 4) each activity has been hyperlinked to its respective desk procedure; and 5) each activity has identified each staff member involved in the process.				
5.0	Have policies and procedures designed to support the achievement of process objectives been established or revised, communicated, and practiced so that people understand what is expected of them and the scope of their freedom to act?				

Appendix III

DIVISION NAME: _____

PROGRAM NAME: _____

SIGNIFICANT PROCESS — Refer to Division-wide Process Register

ASSESSMENT COMPLETION DATE: _____

6.0	A change management process has been established to ensure that documentation is kept up-to date as processes and controls change.			
7.0	Process and control documentation is promptly updated throughout the year and not just when testing starts.			

Section III - Risk Control Worksheet

Section III is designed to document review of significant risks, risk scores and internal controls to ensure accuracy, completeness, and currency.

		Yes	No	N/A	Comments
1.0	**New Risks (**Not previously identified) - Risks arising from changes in laws and regulations, personnel , Information Systems, conflicts of interest (staff and/or sponsor) duplicate draw requests, documentation lost, kick backs (inspectors, or program staff), unavailability of staff, etc. that could inhibit achievement of program goals and objectives have been identified and risk scores assigned.				
2.0	**Existing Risks (**Previously identified**)** - Inherent risk scores (Inherent risk is risk absent any management activity or controls to prevent an event from happening) have been reviewed and modified as appropriate.				
3.0	**Existing Risk (**Previously identified) Residual risk scores (Residual risk is the level of risk that remains after management has a plan in place to deal with the risk.) have been reviewed and modified as appropriate.				
4.0	Where residual risk scores are not within appetite, key control(s) have been proposed and/or implemented which reduce the risk to within appetite.				
5.0	Fraud risks to which the program are exposed to have been evaluated.				
6.0	All program staff have participated in this risk assessment process.				
7.0	Management has tested the operating effectiveness of primary key controls for all inherent risks that are high or medium impact and possible or reasonably probable to				
8.0	Management has tested operating effectiveness of control environment and information and communication component of SC Housing's internal control system where survey results gave rise to proposed actions to mitigate negative survey responses.				

Section IV - Control Self-Assessment Action Plan

Section IV is designed to document review of the division's control self-assessment action plan to ensure accuracy, completeness, and currency of list of actions planned.

	Yes	No	N/A	Comments

Appendix III

DIVISION NAME: _____
PROGRAM NAME: _____
SIGNIFICANT PROCESS: Refer to Division-wide Process Register
ASSESSMENT COMPLETION DATE: _____

1.0	Control self-assessment action plan has been updated consistent with the results of Section III, 1.0 above. (Note: CSA Action Plan should be updated to separately reflect the results of each annual self-assessment.			
2.0	Management has taken or planned appropriate corrective actions related to reports from external sources for their implications for ERM and such action included in the action plan.			
3.0	passed and "No" or "Some" action taken, as of the date of latest Status Report are explained in the comment section of the action plan.			

Section V - Staff Training

Section V is designed to document management's review of the division's mission, and objectives for accuracy, currency, and completeness.

		Yes	No	N/A	Comments
1.0	Have all new Program/Division Staff (any staff member not attending the CSA Workshops facilitated by IA) members been provided a CSA Participant Guide for their information and review?				
2.0	All staff participating in the Internal Audit facilitated CSA workshops receive annual refresher training				

Section VI - Management's Self-Assessment Report

Section VI is designed to document management's reporting package requirements

		Yes	No	N/A	Comments
1.0	Internal Audit reviewed the division's self-assessment report prior to its issuance to Executive management.				
2.0	Management has included documentation of their division-wide risk assessment, including Risk/Control Worksheets, Control Self-Assessment Action Plan, Internal Audits' report and this checklist with the self-assessment report to Executive management.				
3.0	Other				

CONTROL DEFICIENCIES NOTED:

Summarize the deficiencies noted in internal control testing above.

1
2

CONCLUSION – TEST OF CONTROLS

☐ *Key controls ineffective both individually and in the aggregate to reduce residual risk to within management's acceptable level.*

☐ *Key controls effective either individually or in the aggregate to reduce residual risk to within management's acceptable level.*

Appendix III

DIVISION NAME: _____

PROGRAM NAME: _____

SIGNIFICANT PROCESS

Refer to Division-wide Process Register

ASSESSMENT COMPLETION DATE: _____

☐ *Monitoring controls ineffective both individually and in the aggregate to ensure key controls are operating effectively.*

☐ *Monitoring controls effective both individually and in the aggregate to ensure key controls are operating effectively.*

Annual Control Self-Assessment

Example: Division Director Memo initiating Annual Control Self-Assessment

---

Date: XXXXX 2014
To: **Division Staff**
Cc: **Deputy Director for Programs, Divisional Risk Officer, Director of Internal Audit**
From: **Division Director**
Re: Annual Control Self-Assessment on the Design Adequacy and Effectiveness of Internal Control over **Name of the Division** Significant Processes

Background

Name of the Division self-assessed the design adequacy of its internal control over its significant processes as of _____201x (Ref. Control Self-Assessment Report) in relation to criteria established in "Internal Control--Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission. The objective of that control self-assessment, facilitated by Internal Audit Division, was to ensure that **Name of Division** internal control is properly designed to manage risks which threaten our business objectives to within a prudently acceptable level, or risk appetite. The self-assessment encompassed the control activities for **Name of the Division's** significant processes affecting its programs (List programs) as well as the control environment and information and communication affecting those processes.

During this initial self-assessment, we identified **number of** risks associated with our significant processes. We determined that XX (xx%) of the **number of** risks were managed with properly designed controls to within the risk appetite. In response to the **number of** risks remaining above risk appetite **Name of the Division** developed xx proposed actions for the implementation of new key controls and/or improvement in the design of existing key controls (Attachment ___CSA Action Plan). Additionally, we assessed the control environment and information and communication relative to **Name of Division**'s operations through staff surveys and group discussion of survey results. Based upon our assessment we developed two proposed actions to improve the control environment and information and communication relative to our operations.

Objectives and Scope

In our initial control self-assessment **The Name of the Division** determined the desired capabilities for managing risks identified and implemented proposed corrective actions to remedy noted deficiencies (Attachment III CSA Action Plan) —we have answered the question "Is internal control adequately designed? However, we must be vigilant about

improving them continuously as facts and circumstances change and the risk of external and internal events occurring in the future evolves. In the face of such changes, we need to periodically reassess the internal control adequacy as well as answer the question "Is internal control properly executed?" In order to answer this second question, controls must be tested.

The objective of **The Name of the Division's** annual control self-assessment is to provide reasonable assurance regarding the achievement of objectives in the following categories

- Effectiveness and efficiency of operations (including the safeguarding of assets against unauthorized acquisition, use, or disposition);
- Reliability of program reporting; and
- Compliance with applicable laws and regulations;

Reasonable assurance is a high but not an absolute level of assurance. Control self-assessment allows us to consider the extent to which potential events have an impact on achievement of objectives and to mitigate the risk of events that could have a negative impact. Lastly, the control self-assessment allows us the opportunity to evaluate proposed actions to improve the control environment and information and communication relative to our operations.

I have designated **Staff Name** as the Divisional Risk Officer (DRO) for **the name of Division** and charged **him or her** with responsibility for coordination and documentation of this "annual management driven control self-assessment". **Name of DRO** will be contacting **The Name of the Division** managers ("Process Owner") within the coming week(s) to outline the detailed steps and responsibilities for performance of this self-assessment across **The Name of the Division** operations.

Finally, as Director **The Name of the Division's** I encourage you and your staff to actively participate in performing a thorough control self-assessment, and to take steps necessary to ensure that internal control within **The Name of the Division** remain adequately designed, properly executed, and effective.

Sincerely,

Name

Division Director,

Annual Control Self-Assessment

Example: Divisional Risk Officer Memo Initiating Annual Control Self-Assessment

---

Date: XXXXX 2014

To: **Division Managers**

Cc: **Division Director, Deputy Director for Programs, Director of Internal Audit**

From: **Divisional Risk Officer (DOR)**

Subject: Annual Control Self-Assessment on the Design Adequacy and Effectiveness of Internal Control over **Name of the Division** Significant Processes;
Re: Memorandum to Division Managers, dated_____ from **Division Director;** Same subject

A comprehensive risk management framework provides an end-to-end link between objectives, strategy, and execution of strategy, risks, controls, and assurance across all levels in an organization. Pursuant to the above referenced memorandum, I have been charged with responsibility for coordination and documentation of **The Name of the Division's** first annual management driven control self-assessment. In our initial control self-assessment, facilitated by Internal Audit, we determined the desired capabilities for managing risks identified and implemented proposed corrective actions to remedy noted deficiencies—we answered affirmatively the question "Is internal control adequately designed? Notwithstanding, we must be ever vigilant about improving them continuously as facts and circumstances may change and the risk of external and internal events occurring in the future evolves. In the face of such changes, we need to periodically reassess the internal control adequacy as well as answer the question "Is internal control properly executed. This then is the objective of our annual control self-assessment—that is reassessing internal control adequacy and evaluation of internal control effectiveness.

To this end, and in consultation with IA have outlined below the specific steps for performance of our annual control self-assessment.

Step 1 – *Mission, Objective, & Process Review and Update* – Each division manager along with the division director should review the division's MOP (Mission, Objectives, and Significant Processes) to ensure that the division mission, objectives, and significant processes and process owners are current, accurate and complete and have been effectively communicated to all division staff.

Step 2 – *Process Outlines Review and Update* – Responsible process owner(s), manager or division director should review their respective processes to ensure that they are current, accurate and complete and that they have been effectively communicated to staff.

Step 3 – *Desk Procedures* – Desk procedures have been developed and/or updated to ensure consistency with Process outlines and have been effectively communicated to staff.

Step 4 – *Division-wide Process Register Review and Up*date (where applicable) – Each division manager along with the division director should review the Division-wide Process Register to ensure: 1) all activities listed agrees with the division MOP; 2) all Process Tab #s have been Hyperlinked to the respective Process Outline; 3) all RCW Tab #s have been Hyperlinked to the respective RCW; 4) each activity has been hyperlinked to its respective Desk Procedure; and 5) each activity has identified each staff member involved in the process.

Step 5 – *Risk control worksheets (RCW) Review and Update* – Each division manager along with the division director should review their respective RCWs to ensure 1) process objectives, risks to achieving objectives, and control activities necessary to mitigate risks (key controls) are current, accurate, and complete; 2) Risk scores both inherent and residual are reasonable and residual scores are within SC Housing's risk appetite; 3) control activities have been proposed for risks having residual scores above our risk appetite; and 4) primary key controls have been identified for testing.

Step **6** – *Staff Training* – Each division manager should review with all new staff members the "Control Self-Assessment (CSA) Workshop Participant's Guide and CSA Participant's Workbook in lieu of having attended the IA facilitated CSA workshops; all other staff should receive

Step 7 – *Control Self-Assessment Action Plan Review and Update* – The Divisional Risk Officer (DRO) will ensure the CSA Action Plan is updated to reflect new action items resulting from reviews performed in step 5 above.

Step 8 – *Test of Internal Control effectiveness* – The DRO will in collaboration with division management, identify primary internal controls for testing effectiveness. Factors to be considered include: Significance of risk score, and the strength of the control necessary to reduce the risk within appetite; how long the control has been in operation, how long personnel have been performing the activity, etc.

Step 9 – *Report to Executive Management on the Design Adequacy and Operating Effectiveness of Internal Control over* ***Name of Division*** *Significant Processes* – After DRO's tests of internal control and documentation of results the DRO prepare report for Division Director for submission to Executive Management.

The accompanying Control Self-Assessment Checklist must be used to document your self-assessment as outlined above in steps 1- 9.

If you require additional information or clarification concerning any of these matters, please do not hesitate to contact the undersigned.

Sincerely,

Divisional Risk Officer

Name

Attachment I – Annual Control Self-Assessment Checklist (Refer to Appendix III)

Annual Control Self-Assessment

Example: Divisional Risk Officer Memo Initiating Internal Controls Testing Phase

Date: XXXXX 2014

To: **Division Managers**

Cc: **Deputy Director for Programs, Division Risk Officer, Director of Internal Audit**

From: **Divisional Risk Officer**
Subject: Annual Control Self-Assessment on the Design Adequacy and Effectiveness of Internal Control over **Name of the Division** Significant Processes
Re: Memorandum to Division Manager, dated_____ from Division **Risk Officer**; Same subject

As you are aware, during the "Review Phase" of Name **of the Division's** control self-assessment we identified "key controls" for each risk associated with a process or activity. This first phase of the CSA was primarily aimed at ensuring that internal control is properly designed to manage risks which threaten business objectives to within our risk appetite. The self-assessment did not include "tests" to determine the operating effectiveness of internal control. In consultation with Internal Audit I am initiating the "Testing Phase" of **Name of the Division**'s self-assessment to determine the operating effectiveness of internal control.

I have reviewed the controls with IA and we agree that it is not prudent or practical to attempt to tests every control. Instead, we have decided that only "Primary" key control(s) need be tested. (Primary control is the predominate control activity that reduces the risk score relative to all control activities that reduce the risk score to within our appetite.) In some cases there will be more than one primary key control. Once the primary controls have been identified, I will, in consultation with IA determine how to test those controls (i.e. reviewing files, inquiry of staff, inspection, etc.)

Currently, I am reviewing the "Risk Control Worksheets" (RCWs) for each of the **Name of the Division's** significant process and identifying what I believe are the "primary key controls". I am marking those controls ☑. Once I complete a program/section review, I will contact the program manager to review the results for manager's concurrence, or selection of different "primary key control".

I have completed and attached the RCWs for **Program name** and request that **Name of Program Manager** review each significant process and for each risk that I have identified a primary key control. If you concur with my assessments, respond accordingly, otherwise please indicate your preference as to the primary key control and let's discuss.
Please be sure to review each worksheet in the RCW if you have any questions, please let me know.

Sincerely,

Name

Divisional Risk Officer

Process Outline

Prepared By: **Program/Support Area:** **Owner:**

Date: **Process Name:** **Updated:**

	Process Step	Who	Why	When	Where	How	Applications	Input	Output	Description
1										
2										
3										
4										
5										
6										
7										

Process Outline

Prepared By: **Program/Support Area:** **Owner:**

Date: **Process Name:** **Updated:**

	Process Step	Who	Why	When	Where	How	Applications	Input	Output	Description
1										
2										
3										
4										
5										
6										
7										

Process Outline

Prepared By: **Program/Support Area:** **Owner:**

Date: **Process Name:** **Updated:**

	Process Step	Who	Why	When	Where	How	Applications	Input	Output	Description
1										
2										
3										
4										
5										
6										
7										

Risk/Control Worksheet

Program/Support Area: | Owner: _____ | Appendix VIII

Prepared By: | Process or Activity: | Updated by Own _____

Date:

Key Control ✓

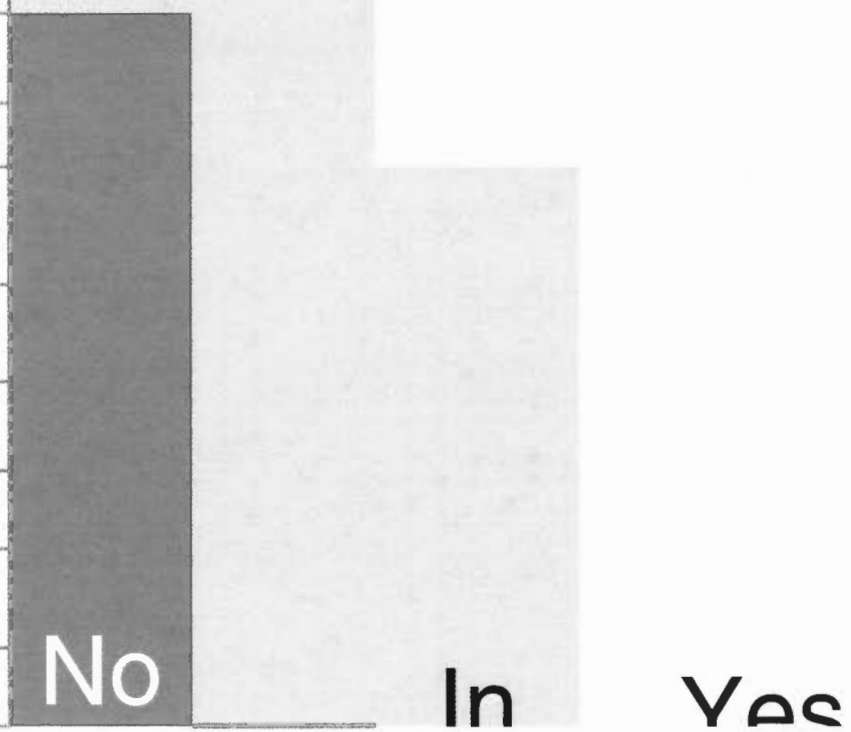
Primary Control ☑

Type of Objective	Process Objectives	Risk #	Risk	Risk Scores (assuming no key controls)			Key Control	Key Control	Key Control	Key Control	Residual Risk Scores			Residual Risk Score within Risk Appetite?	Proposed Key Control	Adjusted Residual Risk Scores		
Strategic, Operations, Reporting, Compliance				Consequence	Likelihood	Significance					Consequence	Likelihood	Significance	Risk Appetite = 4 or less		Consequence	Likelihood	Significance
Proposed Key Control to be implemented by:																		
Scheduled Implementation Date:																		
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
						0							0	Yes				
Monitoring Controls																		
Proposed Monitoring Control:																		
Proposed Monitoring Control to be implemented by:																		
Scheduled Implementation Date:																		
Test of Controls																		
Tested By																		
Date Tested																		
Controls Effective?																		

Appendix IX

Risk Maturity Assessment Tool

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test
Key characteristics (See IIA statement *Risk Based Internal Auditing*)	No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations	Core IA roles (described below) are in brackets - see IIA statement *The Role of Internal Audit in Enterprise-wide Risk Management*
Process						
Are the organization's objectives defined?						Check the organization's objectives are determined by the board and have been communicated to all staff. Check other objectives and targets are consistent with the organization's objectives. (1)
Have management been trained to understand what risks are, and their responsibility for them?						Interview managers to confirm their understanding of risk and the extent to which they manage it. (1)
Has a scoring system for assessing risks been defined?						Check the scoring system has been approved, communicated and is used. (2)
Have processes been defined to determine risks, and these have been followed?						Examine the processes to ensure they are sufficient to ensure identification of all risks. Check they are in use, by examining the output from any workshops. (1)
Have all risks been collected into one list? Have risks been allocated to specific job titles?						Examine the 'Risk Universe'. Ensure it is complete, regularly reviewed, assessed and used to manage risks. Risks are allocated to managers. (1)
Have all risks been assessed in accordance with the defined scoring system?						Check the scoring applied to a selection of risks is consistent with the policy. Look for consistency (that is, similar risks have similar scores). (2)
Have responses to the risks (e.g. controls) been selected and implemented?						Examine the risk register to ensure proper controls should be in place. (3)
Have management set up controls to monitor the proper operation of key controls?						For significant risks, examine the control(s) treating it and ensure management would know if the control failed. (5)
Are risks regularly reviewed by the organization?						Check for evidence that a thorough review process is regularly carried out. (1)



Risk Maturity Assessment Tool

	Risk naïve	Risk aware	Risk defined	Risk managed	Risk enabled	Audit test
Key characteristics (See IIA statement *Risk Based Internal Auditing*)	No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated. Risk appetite defined	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations	Core IA roles (described below) are in brackets - see IIA statement *The Role of Internal Audit in Enterprise-wide Risk Management*
Process						
Has the risk appetite of the organization been defined in terms of the scoring system?						Check the document on which the controlling body has approved the risk appetite. Ensure it is consistent with the scoring system and has been communicated. (1)
Have management reported risks to directors where responses are not managing the risks to a level acceptable to the board?						For risks above the risk appetite, check that the board has been formally informed of their existence. (4)
Are all significant new projects routinely assessed for risk?						Examine project proposals for an analysis of the risks which might threaten them. (1)
Is responsibility for the determination, assessment, and management of risks included in job descriptions?						Examine job descriptions. Check the instructions for setting up job descriptions. (1)
Do managers provide assurance on the effectiveness of their risk management?						Examine the assurance provided. For key risks, check that controls and the management system of monitoring, are operating.(4)
Are managers assessed on their risk management performance?						Examine a sample of appraisals for evidence that risks management was properly assessed for performance. (1)